Discrete Mathematics 20 (1977) 21–31.

THE WEIGHT ENUMERATOR POLYNOMIALS OF SOME CLASSES OF CODES WITH COMPOSITE PARITY-CHECK POLYNOMIALS

Tor HELLESETH
Matematisk Institutt, avd. A, Universitetet i Bergen, 5014 Bergen, Norway

Received 5 January 1976
Revised 30 November 1976

We find the Hamming weight distribution of some classes of linear codes. The cyclic codes in these classes have composite parity-check polynomials.

1. Introduction

Let $F = \mathrm{GF}(q)$, and let F^k be a k-dimensional vector space over F. Elements of F^k are regarded as column vectors of length k. Let $\boldsymbol{G}$ be a $k \times n$ generator matrix for a linear code V of block length n and dimension k over $\mathrm{GF}(q)$. Such a code will be called an $[n, k]$ code over $\mathrm{GF}(q)$.

In this paper we find the Hamming weight enumerators of an infinite number of linear codes. The codes which are investigated here include a class of codes whose Hamming weight enumerator polynomials have earlier been found by Oganesyan, Yagdzyan, and Tairyan [6].

The method applied here is related to the method which Helleseth, Kløve, and Mykkeltveit [4], used in obtaining the weight enumerator polynomials of some irreducible cyclic codes.

2. Preliminaries

Let V_1 be an $[n, k]$ code over F which has a $k \times n$ generator matrix $\boldsymbol{G}$. We first give a construction which gives us an infinite class of codes $\hat{V}_l$ over F, which have weight enumerator polynomials which are related in a very nice way. This construction consists of two steps.

Step 1. For every integer $l \geq 1$ we can consider $\boldsymbol{G}$ as a $k \times n$ generator matrix for an $[n, k]$ code over $\mathrm{GF}(q^l)$. We call these codes V_l for $l \geq 1$.

Step 2. Let B be an irreducible cyclic $[(q^l - 1)/(q - 1), l]$ code over $\mathrm{GF}(q)$ where $\gcd(l, q - 1) = 1$. Then every vector has weight q^{l-1}. Also B is isomorphic to the

field $GF(q^l)$. If α is an element of order $(q^l-1)/(q-1)$ such that $\alpha, \alpha^q, \ldots, \alpha^{q^{l-1}}$ are the nonzeros (roots of the parity-check polynomial) of B, the isomorphism can be defined as in Goethals [3]: $b(x) \in B$ maps onto $b(\alpha) \in GF(q^l)$ and $\xi \in GF(q^l)$ maps onto the codeword $(a_0, a_1, \ldots, a_{(q^l-1)/(q-1)-1})$, where

$$a_i = \mathrm{Tr}_1^l(\xi\alpha^{-i}) \quad \text{and} \quad \mathrm{TR}_1^l(x) = \sum_{i=0}^{l-1} x^{q^i}.$$

A typical codeword of V_l is $(\delta_0, \delta_1, \ldots, \delta_{n-1})$, $\delta_i \in GF(q^l)$. Map each δ_i onto a vector of length $(q^l-1)/(q-1)$ by the isomorphism described above. Then V_l becomes an $[n(q^l-1)/(q-1), kl]$ code which we call $\hat{V}_l$ and a vector of weight i in V_l becomes a vector of weight $q^{l-1}i$ of $\hat{V}_l$.

Hence, starting from an $[n, k]$ code V_1 over F we have constructed a sequence of $[n(q^l-1)/(q-1), kl]$ codes $\hat{V}_l$ over F via a sequence of $[n, k]$ codes V_l over $GF(q^l)$.

If we let $A_l(z)$ and $\hat{A}_l(z)$ denote the weight enumerator polynomials of V_l and $\hat{V}_l$ respectively we note that

$$\hat{A}_l(z) = A_l(z^{q^{l-1}}). \tag{1}$$

It is therefore easy to find the weight distribution of $\hat{V}_l$ from the weight distribution of V_l.

A very interesting fact is that the weight distribution of the codes V_l are related in a nice way and can be found by considering the generator matrix G only. The following theorem which connects the weight distribution $A_l(z)$ of the various V_l is proved in Helleseth, Kløve, and Mykkeltveit [4].

Theorem 2.1. *Let V_l be an $[n, k]$ code with generator matrix $G = (g_{ij})$, $g_{ij} \in F$. Let $A_l(z)$ denote the weight enumerator polynomial of V_l. Then*

$$A_l(z) = \sum_{i=0}^{n} \sum_{j=0}^{k} A_{ij}(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})z^i,$$

where A_{ij} is the number of $(k-j)$-dimensional subspaces of F^k which contain exactly $n-i$ of the n columns of G.

The case $l = 1$ has been known for some time. See MacWilliams [5].

Note that the A_{ij}'s depend on G only and are independent of l. We can arrange the A_{ij}'s in an array:

i \ j	0	1	$\cdots$	$k-1$	k
0	1	0	$\cdots$	0	0
1	0	A_{11}	$\cdots$	$A_{1,k-1}$	A_{1k}
$\vdots$	$\vdots$				$\vdots$
n	0	A_{n1}	$\cdots$	$A_{n,k-1}$	A_{nk}.

Finding $A_1(z) = 1 + \sum_{i=1}^{n} A_{i1}(q-1)z^i$ is equivalent of finding the first column of the array, (i.e. to find how many $(k-1)$-dimensional subspaces of F^k which contains $n-i$ of the n columns of G). To find $A_2(z)$ we also need to find the second column etc. We also note that $A_l(z)$ is determined for every $l \geq 1$ if we know all $A_1(z), \ldots, A_k(z)$ or A_{ij} for $0 \leq i \leq n$, $0 \leq j \leq k$.

In this paper we will consider generatormatrices of two types $G^{(1)}$ and $G^{(2)}$.

Case 1. We let

$$G^{(1)} = [s_1, s_2, \ldots, s_n], \tag{2}$$

where $s_i = \binom{u}{v}$ and u runs through all nonzero vectors in F^{k_1}, v through all nonzero vectors in F^{k_2}. Thus $k = k_1 + k_2$ and $n = (q^{k_1} - 1)(q^{k_2} - 1)$.

Case 2. We let

$$G^{(2)} = [s_1, s_2, \ldots, s_n], \tag{3}$$

where $s_i = \binom{u}{v}$ and u runs through $S_1 \subset F^{k_1}$ where S_1 has the property that every subset of k_1 vectors from S_1 contains k_1 linearly independent vectors v through all nonzero vectors in F^{k_2}. Thus $k = k_1 + k_2$ and $n = n_1(q^{k_2} - 1)$ where $|S_1| = n_1$.

As above we will construct infinite sequences of codes $\hat{V}_l^{(1)}$ and $\hat{V}_l^{(2)}$ from $G^{(1)}$ and $G^{(2)}$ respectively. In Section 3 we will find the A_{ij}'s for $G^{(1)}$ and $G^{(2)}$. Using Theorem 2.1 and (1) we find $\hat{A}_l(z)$ for every $l \geq 1$ in the two cases above.

Let $\mathcal{F}^k$ denote the family of subspaces of F^k. Let $\mathbf{Z}$ denote the set of integers. In Section 3 we need the following results.

Theorem 2.2. *Let f and g be mappings from $\mathcal{F}^k$ into $\mathbf{Z}$. Let $X, U \in \mathcal{F}^k$. If $f(X) = \sum_{\{0\} \subseteq U \subseteq X} g(U)$, then*

$$g(X) = \sum_{\{0\} \subseteq U \subseteq X} (-1)^{\dim X - \dim U} q^{\binom{\dim X - \dim U}{2}} f(U).$$

Lemma 2.3. *Let $\begin{bmatrix} n \\ k \end{bmatrix} = |\{W \in \mathcal{F}^n \mid \dim W = k\}|$. Then*

$$\prod_{i=0}^{n-1} (x - q^i) = \sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} (-1)^i q^{\binom{i}{2}} x^{n-i}.$$

Theorem 2.2, which is the Möbius inversion formula on the lattice $\mathcal{F}^k$, and Lemma 2.3, can be found in Bender and Goldman [1].

Lemma 2.4. *Let $X \in \mathcal{F}^k$, and let*

$$g_l(X) = |\{(v_1, \ldots, v_l) \mid v_i \in F^k \text{ and } \langle v_1, \ldots, v_l \rangle = X\}|.$$

Then we have

$$g_l(X) = \prod_{i=0}^{\dim X - 1} (q^l - q^i).$$

Proof. We define $f_j(X)$ such that $f_j(X) = \sum_{\{0\} \subseteq U \subseteq X} g_j(U)$. Then $f_j(X) = |\{(v_1, \ldots, v_j) \mid v_i \in F^k \text{ and } \langle v_1, \ldots, v_j \rangle \subseteq X\}|$, and therefore $f_j(X) = q^{j \dim X}$. By Theorem 2.2 we have

$$g_j(X) = \sum_{\{0\} \subseteq U \subseteq X} (-1)^{\dim X - \dim U} q^{\binom{\dim X - \dim U}{2}} q^{j \dim U}$$

$$= \sum_{t=0}^{n} \begin{bmatrix} n \\ t \end{bmatrix} (-1)^{n-t} q^{\binom{n-t}{2} + jt},$$

where $n = \dim X$. Hence we have

$$g_j(X) = \sum_{t=0}^{n} \begin{bmatrix} n \\ n-t \end{bmatrix} (-1)^{n-t} q^{\binom{n-t}{2} + jt}$$

$$= \sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} (-1)^{i} q^{\binom{i}{2} + j(n-i)}.$$

By Lemma 2.3 we get

$$g_j(X) = \prod_{i=0}^{\dim X - 1} (q^j - q^i),$$

which was to be proved.

3. Determination of A_{ij}

Let $\mathcal{F}_j^k$ denote the family of j-dimensional subspaces of F^k, with $\mathcal{F}^k = \bigcup_{j=0}^{k} \mathcal{F}_j^k$.

Let $k = k_1 + k_2$. When we write $s = \binom{u}{v}$, we let $u \in F^{k_1}$ and $v \in F^{k_2}$.

Let $W \in \mathcal{F}^k$. We define $U_W = \{u \mid \binom{u}{v} \in W\} \in \mathcal{F}_{j_1}^{k_1}$ and $T_W = \{t \mid \binom{0}{t} \in W\} \in \mathcal{F}_{j_2}^{k_2}$. It is then easy to see that

$$\binom{u_1}{v_1}, \ldots, \binom{u_{j_1}}{v_{j_1}}, \binom{0}{t_1}, \ldots, \binom{0}{t_{j_2}} \tag{4}$$

is a basis for W whenever $u_1, \ldots, u_{j_1}$ and $t_1, \ldots, t_{j_2}$ are bases for U_W and T_W respectively and $\binom{u_1}{v_1}, \ldots, \binom{u_{j_1}}{v_{j_1}} \in W$.

Note that $\binom{u}{v} \in W$ and $\binom{u}{v'} \in W$ implies that $\binom{0}{v-v'} \in W$ and therefore $v - v' \in T_W$.

Let $W, W' \in \mathcal{F}^k$. It is then straightforward to check the following:

Lemma 3.1. *We have $W = W'$ if and only if $U_W = U_{W'}$, $T_W = T_{W'}$, and $v_i - v_i' \in T_W = T_{W'}$ for $i = 1, 2, \ldots, j_1$.*

This means that when W runs through $\mathcal{F}^k$, then $U_W, T_W, v_1, v_2, \ldots, v_{j_1}$ run through all combinations with $U_W \in \mathcal{F}^{k_1}$, $T_W \in \mathcal{F}^{k_2}$ and every v_i runs through a complete set of representatives of F^{k_2}/T_W for $i = 1, 2, \ldots, j_1$.

Let G_1 be a $k_1 \times n_1$ matrix with components from F, let S_1 denote the set of column vectors of G_1, and let $n_1 = |S_1|$.

Let G be the $k \times n_1(q^{k_2}-1)$ matrix with components from F such that

$$G = [s_1, s_2, \ldots, s_n],$$

where $s_i = \binom{u}{v}$ and u, v run through all possible combinations $u \in S_1$, $v \in F^{k_2} - \{0\}$. We let S denote the set of column vectors of G.

If S_1 consists of all nonzero vectors in F^{k_1}, then $G = G^{(1)}$ as defined in (2).

If S_1 has the property that every set of k_1 vectors from S_1 are linear independent, then $G = G^{(2)}$ as defined in (3). Note that in this case G_1 is the generatormatrix of an $[n_1, k_1]$ maximum distance separable code.

In this section we find the A_{ij}'s of Theorem 2.1 for $G^{(1)}$ and $G^{(2)}$. To simplify notations we let $B_{ij} = A_{n-i,k-j}$. Hence $B_{ij} = |\{W \in \mathcal{F}_j^k \mid |W \cap S| = i\}|$. We let $B_{ij}^* = A_{n_1-i,k_1-j}^*$ where A_{ij}^* refers to G_1.

Using the basis for $W \in \mathcal{F}_j^k$ given in (4) we get:

Lemma 3.2. *We have*

$$|W \cap S| = |U_w \cap S_1| q^{j_2} - \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \in T_w \right\} \right|.$$

Proof. By (4) we get

$$\begin{aligned}
|W \cap S| &= \left| \left\{ a \in F^{j_1}, b \in F^{j_2} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i + \sum_{i=1}^{j_2} b_i s_i \neq 0 \right\} \right| \\
&= \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \in T_w \right\} \right| (q^{j_2}-1) \\
&\quad + \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \notin T_w \right\} \right| q^{j_2} \\
&= \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \right\} \right| q^{j_2} \\
&\quad - \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \in T_w \right\} \right| \\
&= |U_w \cap S_1| q^{j_2} - \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \in T_w \right\} \right|,
\end{aligned}$$

which was to be proved.

Theorem 3.3. *Let $G^{(1)}$ be as in (2). Then*

$$B_{ij} = \sum_{j_1=0}^{k_1} \begin{bmatrix} k_1 \\ j_1 \end{bmatrix} \begin{bmatrix} k_2 \\ j - j_1 \end{bmatrix} \sum_{\rho=0}^{j_1} \begin{bmatrix} k_2 - j + j_1 \\ \rho \end{bmatrix} \prod_{t=0}^{\rho-1} (q^{j_1} - q^t), \qquad i = q^j - q^{j-j_1} - q^{j_1-\rho} + 1.$$

Remark. Note that the expression for B_{ij} contains at most two nonzero terms and is therefore easy to calculate

Proof. Since, in this case, S_1 consists of every nonzero vector of F^{k_1} we get by Lemma 3.2 when $W \in \mathcal{F}_j^k$:

$$|W \cap S| = |U_W \cap S_1| q^{j_2} - \left| \left\{ a \in F^{j_1} \,\middle|\, \sum_{i=1}^{j_1} a_i u_i \in S_1 \text{ and } \sum_{i=1}^{j_1} a_i v_i \in T_W \right\} \right|$$

$$= (q^{j_1} - 1) q^{j_2} - \left| \left\{ a \in F^{j_1} - \{0\} \,\middle|\, \sum_{i=1}^{j_1} a_i v_i \in T_W \right\} \right|$$

$$= q^j - q^{j_2} - q^{j_1 - \dim\langle \bar{v}_1, \ldots, \bar{v}_{j_1} \rangle} + 1,$$

where $\bar{v}_i = v_i + T_W \in F^{k_2}/T_W$.

By Lemma 3.1 we note that when W runs through $\mathcal{F}_j^k$, then U_W, T_W, and $\bar{v}_i$ run through all combinations $U_W \in \mathcal{F}_{j_1}^{k_1}$, $T_W \in \mathcal{F}_{j_2}^{k_2}$, and $\bar{v}_i \in F^{k_2}/T_W$ for $i = 1, 2, \ldots, j_1$, such that $j = j_1 + j_2$. The number of $W \in \mathcal{F}_j^k$ such that $\dim U_W = j_1$, $\dim T_W = j_2$, and $\dim\langle \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{j_1} \rangle = \rho$ is therefore

$$\begin{bmatrix} k_1 \\ j_1 \end{bmatrix} \begin{bmatrix} k_2 \\ j_2 \end{bmatrix} \begin{bmatrix} k_2 - j_2 \\ \rho \end{bmatrix} \prod_{i=0}^{\rho-1} (q^{j_1} - q^i),$$

since $\begin{bmatrix} k_1 \\ j_1 \end{bmatrix}$ and $\begin{bmatrix} k_2 \\ j_2 \end{bmatrix}$ are the number of choices of U_W and T_W respectively and $\begin{bmatrix} k_2 - j_2 \\ \rho \end{bmatrix} \prod_{i=0}^{\rho-1} (q^{j_1} - q^i)$ is, by Lemma 2.4, the number of choices of $\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{j_1}$ such that $\dim\langle \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{j_1} \rangle = \rho$. All these choices of W give $|W \cap S| = q^j - q^{j_2} - q^{j_1 + \rho} + 1$. Hence

$$B_{ij} = |\{W \in \mathcal{F}_j^k \mid |W \cap S| = i\}|$$

$$= \sum_{j_1=0}^{k_1} \begin{bmatrix} k_1 \\ j_1 \end{bmatrix} \begin{bmatrix} k_2 \\ j - j_1 \end{bmatrix} \sum_{\rho=0}^{j_1} \begin{bmatrix} k_1 - j + j_1 \\ \rho \end{bmatrix} \prod_{i=0}^{\rho-1} (q^{j_1} - q^i), \qquad i = q^j - q^{j - j_1} - q^{j_1 + \rho} + 1,$$

which was to be proved.

We next will determine B_{ij} for $G^{(2)}$ defined in (3). Then since G_1 is a maximum distance separable code we get

$$B_{ij}^* = \binom{n_1}{i} \sum_{h=0}^{j-i} (-1)^h \binom{n_1 - i}{h} \begin{bmatrix} k_1 - i - h \\ k_1 - j \end{bmatrix} \quad \text{for } j < k_1,$$

$B_{n_1 k_1}^* = 1$ and $B_{i k_1}^* = 0$ when $i < n_1$. See Helleseth, Kløve, and Mykkeltveit [4].

Theorem 3.4. *Let $G^{(2)}$ be as defined in* (3). *Then*

$$B_{ij} = \sum_{j_1=0}^{k_1-1} \begin{bmatrix} k_2 \\ i - j_1 \end{bmatrix} \sum_{\substack{0 \le \gamma \le \rho \le j_1 \\ i = \rho q^{j-j_1} + j_1 - \gamma}} B_{n_1 j_1}^* q^{(j_2 - \rho)(j_1 - \rho)} \binom{\rho}{\gamma} (q^{k_2 - \rho + \gamma} - 1)^{\rho - \gamma}$$

$$+ \begin{bmatrix} k_2 \\ j - k_1 \end{bmatrix} \sum_{\substack{0 \le \gamma \le n_1 \\ i = n_1 q^{j-k_1} + \gamma}} \sum_{r=0}^{k_1} B_{\gamma, k_1 - r}^* \prod_{t=0}^{r-1} (q^{k-j} - q^t),$$

where

$$B_{ij}^* = \binom{n_1}{i} \sum_{h=0}^{j-i} (-1)^h \binom{n_1 - j}{h} \begin{bmatrix} k_1 - i - h \\ k_1 - j \end{bmatrix} \quad \text{for } j < k_1,\ B_{n_1 k_1}^* = 1 \quad \text{and}$$

$$B_{ik_1} = 0 \quad \text{when } i < n_1.$$

Proof. We assume $G_1 = [s_1^*, s_2^*, \ldots, s_{n_1}^*]$, where

$$s_1^* = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, s_2^* = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, s_{k_1}^* = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

For $U \in \mathcal{F}_{j_1}^{k_1}$ we choose a basis $u_1, u_2, \ldots, u_{j_1}$ for U as follows. If $j_1 = k_1$ let $u_1 = s_1^*, u_2 = s_2^*, \ldots, u_{k_1} = s_{k_1}^*$. If $j_1 < k_1$ and $U \cap S_1 = \{s_{i_1}^*, s_{i_2}^*, \ldots, s_{i_\rho}^*\}$, then $s_{i_1}^*, \ldots, s_{i_\rho}^*$ are linear independent and we choose $u_1 = s_{i_1}^*, u_2 = s_{i_2}^*, \ldots, u_\rho = s_{i_\rho}^*$ and let $u_{\rho+1}, u_{\rho+2}, \ldots, u_{j_1}$ be arbitrary such that $u_1, u_2, \ldots, u_{j_1}$ is a basis for U.

Let $W \in \mathcal{F}_{j_2}^{k_2}$. Using the basis in (4) for W we divide $\mathcal{F}_{j_2}^{k_2}$ into two classes depending on $\dim U_W$.

Class 1. Let $\dim U_W = j_1 < k_1$. If we let $|U_W \cap S_1| = \rho$ then we get from Lemma 3.2, since we have chosen the basis for U_W as above

$$|W \cap S| = \rho q^{j_2} - \gamma,$$

where $\gamma = |\{i \mid v_i \in T_W,\ 1 \leq i \leq \rho\}|$. We have $0 \leq \gamma \leq \rho \leq j_1 < k_1$.

The number of $W \in \mathcal{F}_{j_2}^{k_2}$ such that $\dim U_W = j_1$, $|U_W \cap S_1| = \rho$, $\dim T_W = j_2$, and $|\{i \mid v_i \in T_W,\ 1 \leq i \leq \rho\}| = \gamma$ is by Lemma 3.1

$$B_{\rho j_1}^* \begin{bmatrix} k_2 \\ j_2 \end{bmatrix} q^{(k_2 - j_2)(j_1 - \rho)} \binom{\rho}{\gamma} (q^{k_2 - j_2} - 1)^{\rho - \gamma}, \tag{5}$$

since $B_{\rho j_1}^*$ is the number of choices of U_W such that $\dim U_W = j_1$ and $|U_W \cap S_1| = \rho$, $\begin{bmatrix} k_2 \\ j_2 \end{bmatrix}$ is the number of choices of T_W such that $\dim T_W = j_2$, $q^{(k_2 - j_2)(j_1 - \rho)}$ is the number of choices of $v_{\rho+1}, v_{\rho+2}, \ldots, v_{j_1}$, and $\binom{\rho}{\gamma}(q^{k_2 - j_2} - 1)^{\rho - \gamma}$ is the number of of choices of $v_1, v_2, \ldots, v_\rho$ such that exactly γ of these belong to T_W, when every v_i for $i = 1, 2, \ldots, j_1$ runs through a complete set of representatives of F^{k_2}/T_W. Every such $W \in \mathcal{F}_{j_2}^{k_2}$ give $|W \cap S| = \rho q^{j_2} - \gamma$.

Class 2. Let $\dim U_W = k_1$. Then our basis for U_W is

$$\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

Hence $S_1 \subseteq U_W$ and $\sum_{i=1}^{k_2} a_i u_i = a$. By Lemma 3.2 we get $|W \cap S| = n q^{j_2} - \gamma$, where $\gamma = |\{a \in S_1 \mid \sum_{i=1}^{k_2} a_i \bar{v}_i = \bar{0}\}|$.

Here $\bar{v}_i = v_i + T_W \in F^{k_2}/T_W$. When v_i runs through a complete set of representatives, then $\bar{v}_i$ runs through the vectorspace F^{k_2}/T_W of dimension $k_2 - j_2$. We consider $\bar{v}_i$ as elements of $F^{k_2-j_2}$ for $i = 1, 2, \ldots, j_1$. Let $V^\perp = \{a \in F^{k_1} | \sum_{i=1}^{k_1} a_i \bar{v}_i = \bar{0}\}$. Then $V^\perp$ is the orthogonal complement of the rowspace of the $(k_2 - j_2) \times k_1$ matrix $[\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{k_1}]$. When $\bar{v}_i$ for $i = 1, 2, \ldots, k_1$ runs through $F^{k_2-j_2}$ independent of each other, then the row vectors r_i of this matrix run through every k_1-dimensional vector independent of each other for $i = 1, 2, \ldots, k_2 - j_2$. By Lemma 2.4 every rowspace of dimension r occurs $\prod_{i=0}^{r-1}(q^{k_2-j_2} - q^i)$ times. Hence every $V^\perp$ of dimension $k_1 - r$ also occurs $\prod_{i=0}^{r-1}(q^{k_2-j_2} - q^i)$ times.

The number of $W \in \mathcal{F}_j^k$ such that $\dim U_W = k_1$, $\dim T_W = j_2$, $\gamma = |V^\perp \cap S_1|$, and $\dim V^\perp = k_1 - r$ is by Lemma 3.1

$$B^*_{\gamma,k_1-r} \prod_{i=0}^{r-1} (q^{k_2-j_2} - q^i) \begin{bmatrix} k_2 \\ j_2 \end{bmatrix}. \tag{6}$$

since $\begin{bmatrix} k_2 \\ j_2 \end{bmatrix}$ is the number of choices of T_W such that $\dim T_W = j_2$, and B^*_{γ,k_1-r} is the number of $V^\perp$ such that $\dim V^\perp = k_1 - r$ and $\gamma = |V^\perp \cap S_1|$. Since $V^\perp$ runs through $\mathcal{F}^{k_1}_{k_1-r}$ exactly $\prod_{i=0}^{r-1}(q^{k_2-j_2} - q^i)$ times when every v_i for $i = 1, 2, \ldots, k_1$ runs through a complete set of representatives of F^{k_2}/T_W, we get (6). Every such $W \in \mathcal{F}_j^k$ give $|W \cap S| = n_1 q^{j_2} - \gamma$.

Since every $W \in \mathcal{F}_j^k$ belongs to class 1 or class 2 we get Theorem 3.4 when we combine (5) and (6).

4. Applications

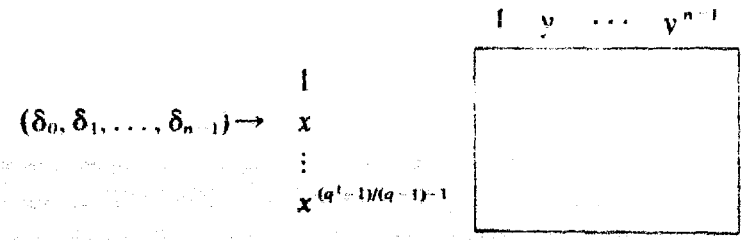
In this section we will apply the results obtained in Sections 2 and 3, and we will find the Hamming weight enumerator polynomials of some cyclic codes which have composite parity-check polynomials, and whose weight enumerator polynomials have not been reported earlier except in a few cases.

Using Theorem 2.1, Theorem 3.3, Theorem 3.4, and (1) we are able to construct a sequence of codes $\hat{V}_l$, $l \geq 1$, with known weight distribution, starting from a code V_1 with generator matrix $G^{(1)}$ or $G^{(2)}$.

We next show that if V_1 is a cyclic $[n, k]$ code then $\hat{V}_l$ can be taken to be a cyclic $[n(q^l - 1)/(q - 1), kl]$ code over F when $\gcd(n, (q^l - 1)/(q - 1)) = 1$.

If V_1 is a cyclic $[n, k]$ code over F with parity-check polynomial $h(x) \in F[x]$, then V_l is a cyclic $[n, k]$ code over $GF(q^l)$ with $h(x)$ as parity-check polynomial for every $l \geq 1$.

If V_l is a cyclic code, and n and $(q^l - 1)/(q - 1)$ are relatively prime, the code $\hat{V}_l$ can be arranged as a cyclic code as follows: Let $(\delta_0, \delta_1, \ldots, \delta_{n-1}) \in V_l$, map each δ_i onto a column vector of length $(q^l - 1)/(q - 1)$ and weight q^{l-1} by the isomorphism described in Section 2. The codeword $(\delta_0, \delta_1, \ldots, \delta_{n-1})$ becomes a $(q^l - 1)/(q - 1) \times n$ array



Label the rows of this array by $1, x, \ldots, x^{(q^l-1)/(q-1)-1}(x^{(q^l-1)/(q-1)} = 1)$ and the columns by $1, y, \ldots, y^{n-1}(y^n = 1)$. A codeword of $\hat{V}_l$ is then $f(x, y)$ a polynomial in x and y.

Set $xy = z$. For each $s, t, 0 \leq s \leq (q^l - 1)/(q - 1) - 1$, $0 \leq t \leq n - 1$ there is a unique $r, 0 \leq r \leq n(q^l - 1)/(q - 1) - 1$ such that $r \equiv s \pmod{(q^l - 1)/(q - 1)}$, $r \equiv t \pmod{n}$, and $z^r = x^s y^t$. Then $f(x, y) = \sum_{j=0}^{(q^l-1)/(q-1)n-1} a_j z^j$, and $(a_0, a_1, \ldots, a_{n(q^l-1)/(q-1)-1})$ is a codeword of the cyclic code $\hat{V}_l$.

If $\alpha, \alpha^q, \ldots, \alpha^{q^{l-1}}$ are the nonzeros of B and $\gamma_1, \gamma_2, \ldots, \gamma_k$ the nonzeros of V_l, then by Berlekamp and Justesen [2] the nonzeros of $\hat{V}_l$ are

$$\alpha\gamma_1, (\alpha\gamma_1)^q, \ldots, (\alpha\gamma_1)^{q^{l-1}}, \ldots, \alpha\gamma_k, (\alpha\gamma_k)^q, \ldots, (\alpha\gamma_k)^{q^{l-1}}.$$

Hence, if V_l is a cyclic code, and $\gcd(n, (q^l - 1)/(q - 1)) = 1$, and $\gamma_1, \gamma_2, \ldots, \gamma_k$ are the nonzeros of V_l, then the nonzeros of $\hat{V}_l$ are $(\alpha\gamma_j)^{q^i}$, $1 \leq j \leq k$, $0 \leq i < l$.

Case 1. Construction of cyclic codes from $\boldsymbol{G}^{(1)}$. Let $\lambda_1, \lambda_2, \ldots, \lambda_{q-1}$ be the nonzero elements of F. Let $\boldsymbol{G}^{(1)} = \lambda_1\boldsymbol{H} \mid \lambda_2\boldsymbol{H} \mid \cdots \mid \lambda_{q-1}\boldsymbol{H}$. If $\gcd(k_1, k_2) = 1$, then $\boldsymbol{H}$ may be taken to be a cyclic code as follows: Let C_1 be a $[(q^{k_1} - 1)/(q - 1), k_1]$ cyclic code with $\gcd(k_1, q - 1) = 1$. Let C_2 be a $[q^{k_2} - 1, k_2]$ cyclic code. Let $\boldsymbol{H}_i$ be a generator matrix for C_i, $i = 1, 2$. Then we can take $\boldsymbol{H}$ as the $(k_1 + k_2) \times ((q^{k_1} - 1)(q^{k_2} - 1))/(q - 1)$ matrix

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{H}_1, \boldsymbol{H}_1, \ldots, \boldsymbol{H}_1 \\ \boldsymbol{H}_2, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_2 \end{pmatrix}.$$

Let now $\boldsymbol{H}$ be the generator matrix of V_1. Let $n = ((q^{k_1} - 1)(q^{k_2} - 1))/(q - 1)$ and let β be a primitive nth root of unity such that $\beta^{q^{k_2}-1}$ is a nonzero of C_1 and $\beta^{(q^{k_1}-1)/(q-1)}$ is a nonzero of C_2. The code generated by $\boldsymbol{H}$ has the $k_1 + k_2$ nonzeros

$$(\beta^{q^{k_2}-1})^{q^i}, \quad (\beta^{(q^{k_1}-1)/(q-1)})^{q^j}, \quad 0 \leq i < k_1, \quad 0 \leq j < k_2.$$

If $\gcd(k_1, k_2) = \gcd(k_1, l) = \gcd(k_2, l) = \gcd(k_1, q - 1) = 1$, then $\gcd(n, (q^l - 1)/(q - 1)) = 1$ and the nonzeros of $\hat{V}_l$ fall in two conjugacy classes

$$(\alpha\beta^{q^{k_2}-1})^{q^i}, \quad (\alpha\beta^{(q^{k_1}-1)/(q-1)})^{q^j}, \quad 0 \leq i < k_1 l, \quad 0 \leq j < k_2 l.$$

Thus the parity check polynomial of $\hat{V}_l$ is a product of two irreducible polynomials of degree $k_1 l$ and $k_2 l$ respectively. Since $\boldsymbol{G}^{(1)}$ and $\boldsymbol{H}$ are closely related, the weight distribution of $\hat{V}_l$ for every $l \geq 1$ can easily be calculated from Theorem 2.1, Theorem 3.3, and (1).

Case 2. Construction of cyclic codes from $\boldsymbol{G}^{(2)}$. Let C_1 be an $[n_1, k_1]$ cyclic maximum distance separable code. Let C_2 be a $[q^{k_2} - 1, k_2]$ cyclic code where $\gcd(n_1, q^{k_2} - 1) = 1$. Let $\boldsymbol{H}_i$ be a generator matrix for C_i, $i = 1, 2$. Then we can take $\boldsymbol{G}^{(2)}$ as the $(k_1 + k_2) \times n_1(q^{k_2} - 1)$ matrix

$$G^{(2)} = \begin{pmatrix} H_1, H_1, \ldots, H_1 \\ H_2, H_2, \ldots, H_2 \end{pmatrix}.$$

Let now $G^{(2)}$ be the generator matrix of V_1. Let $\gamma_1, \gamma_2, \ldots, \gamma_{k_1}$ and $\gamma_{k_1+1}, \gamma_{k_1+2}, \ldots, \gamma_k$ be the nonzeros of C_1 and C_2 respectively, then $\gamma_1, \gamma_2, \ldots, \gamma_k$ are the nonzeros of V_1. Thus we easily find the nonzeros of $\hat{V}_l$ for every $l \geq 1$. The weight distribution of $\hat{V}_l$ can easily be calculated from Theorem 2.1, Theorem 3.4, and (1).

Example. Let $q = 2$, $k_1 = 1$, $k_2 = 2$, and let

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

be a generator matrix for a [3, 3] code over GF(2). Let B be a [7, 3] code. The isomorphism between B and GF (2^3) can be taken to be

$$1 \leftrightarrow 1\ 1\ 1\ 0\ 1\ 0\ 0,$$

$$\alpha \leftrightarrow 0\ 1\ 1\ 1\ 0\ 1\ 0,$$

$$\alpha^2 \leftrightarrow 0\ 0\ 1\ 1\ 1\ 0\ 1, \quad \text{etc.}$$

Thus the codeword $(1, \alpha, \alpha^2)$ of the [3, 3] code V_3 becomes the array

$$\begin{array}{c} \\ 1 \\ x \\ x^2 \\ x^3 \\ x^4 \\ x^5 \\ x^6 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & y & y^2 \end{array} \\ \left[\begin{array}{ccc} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] \end{array},$$

$f(x, y) = 1 + x + xy + x^2 + x^2y + x^2y^2 + x^3y + x^3y^2 + x^4 + x^4y^2 + x^5y + x^6y^2$. The exponents of x, y, z are shown in the following table

	0	1	2
0	0	7	14
1	15	1	8
2	9	16	2
3	3	10	17
4	18	4	11
5	12	19	5
6	6	13	20

$f(x, y) = 1 + z + z^2 + z^9 + z^{10} + z^{11} + z^{15} + z^{16} + z^{17} + z^{18} + z^{19} + z^{20}$.

The nonzeros of B are $\alpha, \alpha^2, \alpha^4$ where $\alpha^7 = 1$, and of V_3 $1, \beta, \beta^2$ where $\beta^3 = 1$. Let γ be a primitive 21th root of unity with $\alpha = \gamma^3$, $\beta = \gamma^7$. The nonzeros of $\hat{V}_3$ are

$$\gamma^3, \gamma^6, \gamma^{12},$$

$$\gamma^{10}, \gamma^{20}, \gamma^{19}, \gamma^{17}, \gamma^{13}, \gamma^5,$$

which are roots of two irreducible polynomials of degree 3 and 6.

The weight distribution of $\hat{V}_3$ is according to Theorem 3.3 (or Theorem 3.4) and (1)

$$\hat{A}_3(z) = 1 + 21z^4 + 147z^8 + 343z^{12}.$$

Acknowledgment

The author is grateful for the suggestions of the anonymous referee. Due to his critiscism the original version of this paper has been considerably improved.

References

[1] E.A. Bender and J.R. Goldman, On the applications of Möbius inversion in combinational analysis, Amer. Math. Monthly 82 (8) 789–803.

[2] E.R. Berlekamp and J. Justesen, Some long cyclic linear codes are not so bad, IEEE Trans. Inform. Theory 20 (1974) 351–356.

[3] J.M. Goethals, Factorization of cyclic codes, IEEE Trans. Inform. Theory 13 (1967) 242–246.

[4] T. Helleseth, T. Kløve and J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block lengths $n_1(q^l - 1)/N$, Discrete Math. 18 (1977) 179–211.

[5] F.J. MacWilliams, Error correcting codes for multiple level transmission, Bell System Tech. J. 40 (1961) 281–307.

[6] S.S. Oganesyan, V.G. Yagdzyan and V.J. Tairyan, On a class of optimal cyclic codes, in: B.N. Petrov and F. Csaki, eds., 2nd International Symposium on Information Theory (Akadémiai Kiadó, Budapest, 1973).